(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 488 577 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
18.04.2007 Bulletin 2007/16

(21) Application number: **03707963.9**

(22) Date of filing: **18.03.2003**

(51) Int Cl.:
H04L 12/46 *(2006.01)* ***H04L 12/24*** *(2006.01)*

(86) International application number:
PCT/CA2003/000363

(87) International publication number:
WO 2003/079614 (25.09.2003 Gazette 2003/39)

(54) RESOURCE ALLOCATION USING AN AUTO-DISCOVERY MECHANISM FOR PROVIDER-PROVISIONED LAYER-2 AND LAYER-3 VIRTUAL PRIVATE NETWORKS

RESSOURCENZUTEILUNG MIT HILFE EINES AUTOMATISCHEN ERKENNUNGSVERFAHRENS FÜR PROVIDERKONTROLLIERTE SCHICHT-2 UND SCHICHT-3 VIRTUELLE PRIVATE NETZWERKE

AFFECTATION DE RESSOURCES AU MOYEN D'UN MECANISME DE DECOUVERTE AUTOMATIQUE POUR RESEAUX PRIVES VIRTUELS DE COUCHE 2 ET DE COUCHE 3 GERES PAR LE FOURNISSEUR DE SERVICES

(84) Designated Contracting States:
DE FR GB

(30) Priority: **18.03.2002 US 365878 P**

(43) Date of publication of application:
22.12.2004 Bulletin 2004/52

(73) Proprietor: **Nortel Networks Limited**
St Laurent, Québec H4S 2A9 (CA)

(72) Inventors:
- **OULD-BRAHIM, Hamid**
  Kanata, Ontario K2M 2S8 (CA)
- **FEDYK, Donald**
  Groton, MA 01450 (US)

(74) Representative: **Ameline, Jean-Paul B.C. et al**
Nortel Networks Limited, London Road
Harlow, Essex CM17 9NA (GB)

(56) References cited:
US-A- 6 079 020
US-A- 6 085 238
US-B1- 6 473 863

EP 1 488 577 B1

Description

FIELD OF THE INVENTION

[0001] The present invention relates generally to virtual Private Networks (VPNs) and, more particularly, to a technique for implementing resource allocation for implementing VPN services using an auto-discovery process for configuring one or more Layer-2 and Layer-3 VPNs.

BACKGROUND OF THE INVENTION

[0002] In the absence of a privacy mechanism, sensitive data (e.g., passwords, account numbers, proprietary information, etc.) transmitted over a network may be susceptible to interception by unauthorized parties. One privacy mechanism commonly used to protect network data is the Virtual Private Network (VPN). Using specialized tunneling protocols and optionally secure encryption techniques, data integrity and privacy may be maintained in a VPN in what seems like a dedicated point-to-point connection.

[0003] Network-based VPNs typically are implemented through a tunneling mechanism. In general, the tunneling mechanism encapsulates the packet headers and/or payload prior to transmission of the packet over an established VPN tunnel. As a result, the transmission of a VPN-based packet only uses non-tunneling information, such as the Internet Protocol (IP) addresses of the ends of the tunnels, while the sensitive information, such as the source and destination IP addresses and sensitive payload data, remains encapsulated. Exemplary tunneling mechanisms include IP/IP tunneling, Generic Router Encapsulation (GRE) tunneling, IP Security (IPSec) tunneling and Multi-Protocol Label Switching (MPLS) tunneling. The configuration of VPN tunnel typically is specific to the particular type of VPN used.

[0004] A typical Network IP-based VPN generally includes at least two provider edge (PE) devices (e.g., a VPN-enabled router) interconnected via a series of provider devices (e.g., routers) that form a network backbone, where the network backbone typically includes one or more public networks, such as, for example, the Internet or a wide area network (WAN). Connected to each PE device are one or more customer edge (CE) devices, such as a workstation or personal computer. In this type of network-based VPN, VPN tunnels are established between PE devices, rather than between CE devices. These tunnels, herein referred to as PE-PE tunnels, typically are established at either Layer-2 or Layer-3 of the International Standard Organization's Open System Interconnect (ISO/OSI) network model. Exemplary VPN mechanisms at Layer-2 include Virtual Private LAN Service (VPLS) (see Waldemar Augustyn et al., "Requirements for Virtual Private LAN Services (VPLS)," October 2002, available at <http://www.ietf.org/internet-drafts/draft-ietf-ppvpn-vpls-requirement-01.txt>) and Virtual Private Wire (VPW)(see Eric Rosen et al., "L2VPN Framework," February 2003, available at <http://www.ietf.org/internet-drafts/draft-ietf-ppvpn-12-framework-03.txt>). Exemplary VPN mechanisms at Layer-3 include Virtual Routing (VR)-based mechanisms, such as VR using Border Gateway Protocol (EGP) (see Hamid Ould-Brahim et al. "Network based IP VPN Architecture using Virtual Routers," July 2002, available at <http://www.ietf.org/ internet- drafts/ draft- ietf- ppvpn- vpn- vr-03.txt>) or VPNs based on RFC 2547bis (often referred to as BGP/MLPS-based VPNs) (see Eric Rosen et al., "BGP/MPLS VPNs" available at <http://www.ietf.org/internet-drafts/draft-ietf-ppvpn-rfc2547bis-03.txt>, October 2002).

[0005] Regardless of the VPN mechanism used, a primary step in establishing a network-based VPN is to provide information about each VPN configured on a local PE device to the remaining remote PE devices. A number of mechanisms may be implemented to achieve this distribution of PE information, such as BGP, Domain Name Service (DNS), Remote Authentication Dial In User Service (RADIUS), and the like. Such mechanisms are well known in the art. After distributing this PE information, one or more PE-PE tunnels typically are established based in part on information received through a VPN auto-discovery mechanism.

[0006] Various tunnel signalling protocols may be used to establish and maintain VPN tunnels, such as, for example, Resource Reservation Protocol (RSVP), Resource Reservation Protocol - Traffic Engineered (RSVP-TE), Label Distribution Protocol (LDP), Constraint-based Routing LDP (CR-LDP), Asynchronous Transfer Mode (ATM), Frame Relay, Generic Routing Encapsulation (GRE), IPSec, and the like.

[0007] Various parameters for VPN tunnels in conventional Layer-2 and Layer-3 VPNs typically are configured manually by the service provider. As a result, the scalability of such conventional VPN implementations is limited due to the difficulty in manually configuring a complex and dynamic VPN system having a large number of PE devices and/or constantly changing system requirements, such as a continuous changing number of tunnels/VPNs, constant, continuous changes in resources such as bandwidth, delay and/or Quality of Service (QoS) requirements, and the like. Further, these conventional VPN implementations generally lack a defined mechanism to relate VPN tunnels to a per VPN or per set of VPNs resources such as QoS profiles or other tunnel-specific parameters. As a result, the flexibility of such conventional VPN systems is compromised because the VPN is unable to predictably respond to changes in bandwidth requirements, QoS requirements, and the like.

[0008] In view of the foregoing, it would be desirable to provide a technique for facilitating the configuration of VPN tunnels based at least in part on supplied parameters in an auto-discovery manner. More particularly, it would be desirable to implement resource profiles such as Quality of Service (QoS) parameters using a VPN au-

to-discovery as an extension to existing auto-discovery mechanisms in an efficient and cost effective manner.

SUMMARY OF THE INVENTION

[0009] In accordance with one aspect of the present invention, a method for establishing a Virtual Private Network (VPN) tunnel between a first provider edge (PE) device and a second (PE) device of a Provider-Provisioned VPN (PPVPN) is provided. The method comprises advertising at least one tunnel-based parameter to one or more PE devices over a network backbone using an auto-discovery mechanism, the one or more PE devices including at least one of the first and second PE devices and configuring a VPN tunnel between the first and second PE devices based at least in part on the at least one tunnel-based parameter. A computer signal embodied in a carrier wave readable by a computing system and encoding a computer program of instructions for executing a computer process may be used to perform the above method. The invention also provides at least one readable carrier for storing a computer program of instructions configured to be readable by at least one processor for instructing the at least one processor to execute a computer process for performing the above method.

[0010] A Provider-Provisioned Virtual Private Network (PPVPN) system is provided in accordance with another aspect of the present invention. The system comprises auto-discovery means for distributing at least one Virtual Private Network (VPN) tunnel-based parameter to at least a first and second provider edge (PE) devices and tunnel signalling means for configuring a VPN tunnel over a network backbone between the first and second PE devices based at least in part on the at least one tunnel-based parameter.

[0011] The present invention will now be described in more detail with reference to exemplary embodiments thereof as shown in the appended drawings. While the present invention is described below with reference to preferred embodiments, it should be understood that the present invention is not limited thereto. Those of ordinary skill in the art having access to the teachings herein will recognize additional implementations, modifications, and embodiments, as well as other fields of use, which are within the scope of the present invention as disclosed and claimed herein, and with respect to which the present invention could be of significant utility.

[0012] In order to facilitate a fuller understanding of the present invention, reference is now made to the appended drawings. These drawings should not be construed as limiting the present invention, but are intended to be exemplary only.

Figure 1 is a schematic diagram illustrating a Provider-Provisioned Virtual Private Network (PPVPN) system utilizing a VPN auto-discovery mechanism in accordance with at least one embodiment of the present invention.

Figure 2 is a flow diagram illustrating an overview of a VPN auto-discovery mechanism for establishing and/or maintaining a provider-edge-to-provider-edge (PE-PE) tunnel in accordance with at least one embodiment of the present invention.

Figure 3 is a flow diagram illustrating an exemplary implementation of the VPN auto-discovery mechanism of Figure 2 in a RFC 2547bis-based VPN in accordance with at least one embodiment of the present invention.

Figure 4 is a flow diagram illustrating an exemplary implementation of the VPN auto-discovery mechanism of Figure 2 in a Virtual Routing-based VPN in accordance with at least one embodiment of the present invention.

Figure 5 is a flow diagram illustrating an exemplary implementation of the VPN auto-discovery mechanism of Figure 2 in a Layer-2 VPN using a Virtual Private Local Area Network Service (VPLS)-based or VPW-based mechanism in accordance with at least one embodiment of the present invention.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENT(S)

[0013] Figures 1-5 illustrate various exemplary implementations for creating scalable VPN PE-PE tunnels in Level-2 or Level-2 PPVPNs using an auto-discovery mechanism. Information regarding the establishment and/or configuration of a tunnel between two PE devices may be advertised among the PE devices of a network. This information may include, for example, the desired tunnel signalling protocol, the Quality of Service (QoS) profile for the tunnel, the PE tunnel endpoint, membership information, the VPN technology to be used, etc. In at least one embodiment, this information may be advertised as an extension to a conventional auto-discovery mechanism commonly used in VPNs, such as the Border Gateway Protocol (BGP), directory service protocols (e.g., Domain Name Service (DNS), RADIUS), and the like. After distributing this information, a tunnel may be established between the appropriate PE devices based at least in part on the supplied information. Alternatively, the PEs may select an existing tunnel that complies with some or all of the supplied parameters. By implementing an auto-discovery technique to distribute the QoS profile for the purpose of VPN tunnel configuration and/or establishment information, the scalability of the VPN system may be enhanced because the QoS profile of a tunnel may be set according to the requirements of the VPN services, where the information is distributed among the PEs in an automated fashion rather than implemented by manual configuration as conventional VPN systems.

[0014] Referring now to Figure 1, an exemplary PPVPN system 100 implementing a capability discovery mechanism is illustrated in accordance with at least one embodiment of the present invention. In the illustrated

example, the PPVPN system 100 includes PE routers 102, 104 connected via a network backbone 106. Although described herein as VPN-enabled routers, the PE routers 102, 104 may include other appropriate PE devices such as, for example, MPLS/IP Layer-2 switches. The network backbone 106 may include any number of provider network devices interconnected using one or more data link types such as, for example, IP, ATM, Frame Relay (FR), Time Division Multiplexing (TDM), Ethernet, Optical Ethernet, and the like.

[0015] Connected to each PE router 102, 104 is one or more VPN segments, such as VPN segments 142-146 connected to PE router 102 and VPN segments 152-156 connected to PE router 104. Each VPN segment 142-146, 152-156 may include one or more networked customer edge (CE) devices as well as devices to facilitate network connectivity, such as hubs, routers, switches, bridges, and the like. As understood in the art, CE devices may include any of a variety of networked devices, such as personal computers, laptops, workstations, and the like.

[0016] In general, each VPN segment connected to the PE router 102 is a member of the same VPN as a VPN segment connected to the PE Router 104, thereby allowing a VPN to be established between devices on the VPN segments. In the illustrated example, the VPN segments 142, 152 are members of VPN_A, the VPN segments 144, 154 are members of VPN_B, and the VPN segments 146, 156 are members of VPN_C. Although each VPN segment is illustrated in Figure 1 as a member of a single VPN, it will be appreciated that a VPN segment may be a member of a plurality of VPNs. Likewise, a CE device may be a member of a plurality of VPNs and therefore may be a member of more than one VPN segment.

[0017] To facilitate communications between VPN segments, each PE router 102, 104 may include a VPN interface corresponding to a VPN segment. To illustrate, the PE router 102 may include VPN interfaces 122-126 to interface with VPN segments 142-146, respectively, and the PE router 104 may include VPN interfaces 132-136 to interface with VPN segments 152-156, respectively.

[0018] Depending on the VPN technology utilized, the VPN interfaces 122-126, 132-136 may be implemented in any of a variety of ways. For example, if the PPVPN system 100 implements a Layer-3 VPN using Virtual Routing (VR), the VPN interfaces 122-126, 132-136 may include Virtual Routers implemented by the PE routers 102, 104 to provide Virtual Routing between the CE devices on the VPN segments. Virtual Routing and Virtual Routers are well known to those skilled in the art.

[0019] For example, if the PPVPN system 100 implements a Layer-3 VPN using RFC2547bis, the VPN interfaces 122-126, 132-136 may include Virtual Routing and Forwarding (VRF) implemented by the PE routers 102, 104 to provide Virtual Routing and Forwarding tables between the CE devices on the VPN segments. RFC2547bis and Virtual Routing and Forwarding are well known to those skilled in the art.

[0020] Alternatively, if the PPVPN system 100 implements a Layer-2 VPW in accordance with VPW (see, e.g., "L2VPN Framework," supra), the VPN interfaces 122-126, 132-136 may include a Virtual Switching Instance (VSI) implemented by the PE routers 102, 104 to provide Layer-2 attachment circuits between the CE devices on the VPN segments. Layer-2 VPNs and Virtual Switching Instances are well known to those skilled in the art.

[0021] Further, in at least one embodiment, the PE router 102 may include an auto-discovery (AD) component 112 and a tunnel signalling component 116 and the PE route 104 may include an AD component 114 and a tunnel signalling component 118. As discussed in greater detail below, the tunnel signalling components 116, 118 may be adapted to create, configure and/or maintain one or more VPN tunnels 170 between the PE routers 102-104 using one or more tunnel signalling mechanisms. Exemplary tunnel signalling mechanisms implemented by the tunnel signalling components 116, 118 may include, for example, RSVP, RSVP-TE, LDP, CR-LDP, and the like.

[0022] A number of supplied parameters may be used by the tunnel signalling components 116, 118 to create, configure and/or maintain the one or more tunnels 170 between the PE router 102 and the PE router 104. These parameters may include, for example: the type of tunnelling mechanism to be used (i.e., specifying RSVP-TE or CR-LDP); the QoS profile for each tunnel 170; the PE tunnel endpoints for a particular VPN membership; the VPN technology to use (e.g., Layer-3 technology v. Layer-2 technology, 2547bis v. Virtual Routing, etc.) ; and the like. For ease of discussion, this information is collectively referred to herein as VPN Capability Discovery Information (VCDI).

[0023] In conventional PPVPN systems, this information typically is configured manually at each PE router for each VPN membership. In one embodiment, however, the AD component 112 may be adapted to advertise this information to other PE routers on the backbone 106 using an auto-discovery mechanism (described in greater detail below). The AD component 112 then may provide received VCDI information to the tunnel signalling component 116 for use in creating, maintaining, and/or configuring the one or more tunnels 170 associated with the VCDI information.

[0024] The auto-discovery mechanism may be implemented in any of a variety of ways. In at least one embodiment, the auto-discovery mechanism may be implemented as an extension to conventional information distribution protocols, such as BGP, DNS, and RADIUS. To illustrate using BGP, the VCDI information for each of VPN_A, VPN_B, and VPN_C, may be determined and transmitted to the PE routers 102, 104 as profiles 162-166, respectively, as part of a BGP UPDATE 160 transmitted over the backbone 106. Upon receipt of the BGP UPDATE 160, the AD components 112, 114 (each BGP-

enabled in this case) then may extract the profiles 162-166 and supply the VCDI information of the profiles 162-166 to the tunnel signalling components 116, 118 for use in creating, maintaining, and/or configuring the VPN tunnel(s) 170 associated with each VPN. DNS, RADIUS, and other directory service protocols may be extended in a similar manner to distribute VCDI to the PE routers. Accordingly, rather than having to manually configure VPN tunnels at each PE router, the VPN tunnel configuration information (i.e., the VCDI) may be "piggybacked" onto auto-discovery information by extending the auto-discovery protocol to include the transmission of the VCDI information.

[0025] Referring now to Figure 2, an exemplary overview of the VPN tunnel configuration process is illustrated in accordance with at least one embodiment of the present invention. In the illustrated example, the VPN tunnel configuration process 200 initiates at step 202, wherein the VCDI information for a given VPN may be determined. The VCDI information may include information regarding the configuration of one or more VPN tunnels between PE routers for the VPN. For example, the VCDI information may specify the PE tunnel endpoints, community route targets, resource parameters (e.g., minimum bandwidth, maximum delay, committed burst size, committed rate, jitter, error, ownership, physical position, type of transport medium, etc.), topology information, and other parameters utilized by the tunnel signalling mechanisms to establish and/or configure a VPN tunnel.

[0026] At step 204, the VCDI information obtained at step 202 may be advertised to some or all of the PE routers on the backbone. The advertisement of the VCDI information, in one embodiment, includes incorporating the VCDI information into a conventional information distribution protocol. For example, the VCDI information could be incorporated as an extension of BGP and transmitted between PE routers using, for example, a BGP UPDATE transmission. Alternatively, the VCDI information could be formatted and transmitted in accordance with DNS or RADIUS. Multicast-based protocols also may be extended to multicast the VCDI information to some or all of the PE routers over the backbone.

[0027] At step 206, upon receipt of the VCDI information, a PE router may begin negotiating the creation of a VPN (or per VPN) PE-PE tunnel based at least in part on the received VCDI information. As noted above, the creation and configuration of a VPN tunnel is well known in the art (see Hamid Ould-Brahim et al., "Using BGP as an Auto-Discovery Mechanism for Network-Based VPNs," August 2002, available at <http://www.ietf.org/internet-drafts/draft-ietf-ppvpn-bgvpn-auto-03.txt>

[0028] In creating and configuring the VPN tunnel from the VCDI information, any of a variety of tunnelling mechanisms may be used, as appropriate. Examples of such mechanisms include, for example, RSVF-TE, LDP, CR-LDP, and the like. After creating the VPN tunnel, CE devices on the various VPN segments them may utilize the VPN tunnel to transmit data securely between VPN segments.

[0029] Referring now to Figures 3-5, various exemplary implementations of the process 200 of Figure 2 for certain VPN technologies are illustrated in accordance with at least one embodiment of the present invention. Figure 3 illustrates an exemplary implementation of the process 200 for a VPN system implementing a Layer-3 VPN using RFC 2547bis. Figure 4 illustrates an exemplary implementation of the process 200 for a VPN system implementing a Layer-3 VPN using Virtual Routing. Figure 5 illustrates an exemplary implementation of the process 200 for a VPN system implementing a Layer-2 VPN using VPLS or VPW. While exemplary implementations of the process 200 are illustrated for a number of VPN technologies, those skilled in the art, using the guidelines provided herein, may modify the process 200 for various other VPN technologies without departing from the spirit or the scope of the present invention.

[0030] Referring now to Figure 3, an exemplary auto-discovery process 300 for distributing VPN tunnel configuration information in a Layer-3 PPVPN based on RFC 2547bis is illustrated in accordance with at least one embodiment of the present invention. After determining the relevant VCDI information (step 202, Figure 2), the process 300 initiates at step 302, wherein the VCDI information associated with one or more VPN tunnels may be advertised to the AD components of the PE routers (e.g., AD components 112, 114, Figure 1), as discussed above. As noted above, the VCDI information preferably is distributed as an extension of an auto-discovery protocol, such as BGP, DNS, or RADIUS. At step 304, the tunnel signalling component (e.g., tunnel signalling components 116, 118, Figure 1) at a PE router negotiates with the tunnelling mechanism at a corresponding PE router to establish and configure one or more VPN tunnels based at least in part on the supplied VCDI information. This configuration may include, for example, negotiating QoS for the VPN tunnel, setting a minimum or maximum bandwidth for the VPN tunnel, specifying the tunnelling mechanism, and the like. Alternatively, in one embodiment, the tunnel signalling component may select a pre-existing VPN tunnel that complies with some or all of the parameters set forth by in the VCDI information.

[0031] Upon creation and configuration of the VPN tunnel (or selection of a pre-existing tunnel), Virtual Routing Forwarding (VRF) tables may be generated at each PE router. The generation of VRF tables is well known in the art. At step 306, these VRF tables then may be exported to the backbone using, for example, BGP and then distributed to the appropriate PE routers for use in routing VPN traffic through the established tunnel.

[0032] Referring now to Figure 4, an exemplary auto-discovery process 400 for distributing VPN tunnel configuration information in a Layer-3 VPN based on Virtual Routing is illustrated in accordance with at least one embodiment of the present invention. After determining the relevant VCDI information (step 202, Figure 2), the proc-

ess 400 initiates at step 402, wherein VPN IDs are associated with the endpoints of the tunnel to be established/selected. At this point, it typically is not necessary to advertise the VR prefixes/addresses. At step 404, a list of the VPN IDs is included with other VCDI information and this information may be advertised to the AD components of the PE routers (e.g., AD components 112, 114, Figure 1), as discussed above. For Virtual Routing implementations, the VCDI information preferably is distributed as an extension of a BGP Multiprotocol Extension (BGP-MP). Other information distribution protocols, such as DNS, RADIUS, and IP multicasting may be utilized. At this point, it may be appropriate to advertise the VR prefixes/addresses.

[0033] At step 406, the backbone Virtual Router receiving the VCDI information may be adapted to establish and configure one or more VPN tunnels based at least in part on the supplied VCDI information. This configuration may include, for example, negotiating QoS for the VPN tunnel, setting a minimum or maximum bandwidth for the VPN tunnel, specifying the tunnelling mechanism, and the like. Alternatively, in one embodiment, the tunnel signalling component may select a pre-existing VPN tunnel that complies with some or all of the parameters set forth by in the VCDI information. At step 408, the VPN topology information may be advertised in a manner similar to the advertisement of the VCDI information at step 404.

[0034] Referring now to Figure 5, an exemplary auto-discovery process 500 for distributing VPN tunnel configuration information in a Layer-2 PPVPN based on VPLS or VPW is illustrated in accordance with at least one embodiment of the present invention. After determining the relevant VCDI information (step 202, Figure 2), the process 500 initiates at step 502, wherein the VCDI information associated with one or more VPN tunnels is advertised to the AD components of the PE routers (e.g., AD components 112, 114, Figure 1), as discussed above. At this point, it may be unnecessary to exchange Layer-2 VPN services. As noted above, the VCDI information preferably is distributed as an extension of an auto-discovery protocol, such as BGP, DNS, or RADIUS.

[0035] At step 504, the tunnel signalling component (e.g., tunnel signalling components 116, 118, Figure 1) at a PE router negotiates with the tunnelling mechanism at a corresponding router to establish and configure one or more VPN tunnels based at least in part on the supplied VCDI information. This configuration may include, for example, negotiating QoS for the VPN tunnel, setting a minimum or maximum bandwidth for the VPN tunnel, specifying the tunnelling mechanism, and the like. Alternatively, in one embodiment, the tunnel signalling component may select a pre-existing VPN tunnel that complies with some or all of the parameters set forth by in the VCDI information.

[0036] Upon creation and configuration of the VPN tunnel (or selection of a pre-existing tunnel), Layer-2 VPN advertisements may be created at step 506 and distributed using the backbone BGP component (e.g., AD components 112, 114) at step 508.

[0037] At this point, it should be noted that implementing an auto-discovery VPN tunnel configuration process in accordance with the present invention as described above typically involves the processing of input data and the generation of output data to some extent. This input data processing and output data generation may be implemented in hardware or software. For example, specific electronic components may be employed in a node or similar or related circuitry for implementing an auto-discovery component and tunnel signalling component in accordance with the present invention as described above. Alternatively, one or more processors operating in accordance with stored instructions may implement the functions associated with implementing an auto-discovery VPN tunnel configuration process in accordance with the present invention as described above. If such is the case, it is within the scope of the present invention that such instructions may be stored on one or more processor readable media, or transmitted to one or more processors via one or more signals.

[0038] In summary, the invention provides a technique for resource distribution using an auto-discovery mechanism for Provider-Provisioned Layer-2 and Layer-3 Virtual Private Networks. In one particular exemplary embodiment, the technique may be realized by a method for establishing a Virtual Private Network (VPN) tunnel between a first provider edge (PE) device and a second (PE) device of a provider-provisioned VPN. The method comprises advertising at least one tunnel-based parameter to one or more PE devices over a network backbone using an auto-discovery mechanism, the one or more PE devices including at least one of the first and second PE devices. The method further comprises configuring a VPN tunnel between the first and second PE devices based at least in part on the at least one tunnel-based parameter.

[0039] The present invention is not to be limited in scope by the specific embodiments described herein. Indeed, various modifications of the present invention, in addition to those described herein, will be apparent to those of ordinary skill in the art from the foregoing description and accompanying drawings. Thus, such modifications are intended to fall within the scope of the following appended claims. Further, although the present invention has been described herein in the context of a particular implementation in a particular environment for a particular purpose, those of ordinary skill in the art will recognize that its usefulness is not limited thereto and that the present invention can be beneficially implemented in any number of environments for any number of purposes.

Claims

1. A method for establishing a Virtual Private Network

VPN tunnel (170) between a first provider edge PE device (102) and a second PE device (104) of a Provider-Provisioned VPN PPVPN (100) comprising:

advertising at least one tunnel-based parameter to one or more PE devices over a network backbone (106) using an auto-discovery mechanism, the one or more PE devices including at least one of the first and second PE devices; and
configuring a VPN tunnel between the first and second PE devices based at least in part on the at least one tunnel-based parameter.

2. The method as in Claim 1, wherein the auto-discovery mechanism includes one of: a Border Gateway Protocol BGP-based mechanism; a Domain Name Service DNS-based mechanism; and a Remote Authentication Dial In User Service RADIUS-based mechanism.

3. The method as in Claim 2, wherein the at least one tunnel-based parameter is distributed to the one or more PE devices as an extension of an auto-discovery protocol.

4. The method as in Claim 1, wherein configuring the VPN tunnel includes configuring the VPN tunnel using at least one tunnel signalling mechanism.

5. The method as in Claim 4, wherein the at least one tunnel signalling mechanism includes one of: a Resource Reservation Protocol RSVP-based mechanism; a Resource Reservation Protocol-Traffic Engineered RSVP-TE-based mechanism; a Label Distribution Protocol LDP-based mechanism; and a Constraint-based Routing LDP CR-LDP based mechanism.

6. The method as in Claim 1, wherein the at least one tunnel parameter includes one of: a type of tunnelling mechanism; at least one PE tunnel endpoint; at least one community route target; topology information; and at least one resource parameter.

7. The method as in Claim 6, wherein the at least one resource parameter includes one of: minimum bandwidth; maximum delay; committed burst size; committed rate; jitter; error; ownership; physical position and transport medium.

8. The method of Claim 1, wherein configuring the VPN tunnel includes selecting a pre-existing VPN tunnel, the pre-existing VPN tunnel being compliant with the at least one tunnel parameter.

9. A Provider-Provisioned Virtual Private Network PPVPN system comprising:

auto-discovery means for distributing at least one Virtual Private Network VPN tunnel-based parameter to at least a first and second provider edge PE devices (102, 104); and
tunnel signalling means for configuring a VPN tunnel (170) over a network backbone (106) between the first and second PE devices based at least in part on the at least one tunnel-based parameter.

10. The system as in Claim 9, wherein the auto-discovery means is adapted to distribute the at least one tunnel-based parameter as an extension of at least one auto-discovery protocol.

11. The system as in Claim 10, wherein the auto-discovery protocol comprises one of: a Border Gateway Protocol BGP-based mechanism; a Domain Name Service DNS-based mechanism; and a Remote Authentication Dial In User Service RADIUS-based mechanism.

12. The system as in Claim 9, wherein the tunnel signalling means includes one of: a Resource Reservation Protocol RSVP-based mechanism; a Resource Reservation Protocol-Traffic Engineered RSVP-TE-based mechanism; a Label Distribution Protocol LDP-based mechanism; and a Constraint-based Routing LDP CR-LDP based mechanism.

13. The system as in Claim 9, wherein the at least one tunnel parameter includes one of: a type of tunnelling mechanism; at least one PE tunnel endpoint; at least one community route target; topology information; and at least one resource parameter.

14. The system as in Claim 13, wherein the at least one resource parameter includes one of: minimum bandwidth; maximum delay; committed burst size; committed rate; jitter; error; ownership; physical position and transport medium.

15. The system as in Claim 10 comprising:

the network backbone; and
the first and second PE devices each operably connected to the network backbone.

Patentansprüche

1. Verfahren zum Aufbau eines virtuellen privaten Netzwerk-, VPN-, Tunnels (170) zwischen einem ersten Diensteanbieter-Rand-PE-Gerät (102) und einem zweiten PE-Gerät (104) eines von einem Diensteanbieter bereitgestellten VPN, PPVPN, (100), mit den folgenden Schritten:

Ankündigen von zumindest einem Tunnel-baslerten Parameter an eines oder mehrere PE-Geräte über einen Netzwerk-Backbone (106) unter Verwendung eines automatischen Erkennungsmechanismus, wobei das eine oder die mehreren PE-Geräte zumindest eines der ersten und zweiten PE-Geräte einschließen; und
Konfigurieren eines VPN-Tunnels zwischen den ersten und zweiten PE-Geräten zumindest teilweise auf der Grundlage des zumindest einen Tunnel-basierten Parameters.

2. Verfahren nach Anspruch 1, bei dem der automatische Erkennungsmechanismus einen von folgenden Mechanismen einschließt: einen Rand-Überleiteinrichtungs-Protokoll-, BGP-, basierten Mechanismus; einen Domänen-Namensdienst-, DNS- basierten Mechanismus; und einen Fernauthentifizierungs-Elnwähl-Benutzerdlenst-, RADIUS-, basierten Mechanismus.

3. Verfahren nach Anspruch 2, bei dem der zumindest eine Tunnel-basierte Parameter an das eine oder die mehreren PE-Geräte als eine Erweiterung eines automatischen Erkennungs-Protokolls verteilt wird.

4. Verfahren nach Anspruch 1, bei dem die Konfiguration des VPN-Tunnels das Konfigurieren des VPN-Tunnels unter Verwendung von zumindest einem Tunnel-Slgnalisierungsmechanismus einschließt.

5. Verfahren nach Anspruch 4, bei dem der zumindest eine Tunnel-Signalisierungsmechanismus einen von folgenden Mechanismen einschließt: einen Ressourcen-Reservierungs-Protokoll-, RSVP-, basierten Mechanismus; einen Ressourcen-Reservlerungs-Protokoll-Verkehrsauslegungs-, RSVP-TE-, basierten Mechanismus; einen Etikettverteilungs-Protokoll-, LDP-, basierten Mechanismus; und einen Bedingungs-basierten Routenführungs-, LDP-CR-LDP-, basierten Mechanismus.

6. Verfahren nach Anspruch 1, bei dem der zumindest eine Tunnel-Parameter einen von folgenden Parametern einschließt: einen Typ des Tunnelungsmechanismus; zumindest einen PE-Tunnel-Endpunkt; zumindest ein Gemeinschafts-Routen-Zlel; Topologie-Information; und zumindest einen Ressourcen-Parameter,

7. Verfahren nach Anspruch 6, bei dem zumindest eine Ressourcen-Parameter einen von folgenden Parametern einschließt: minimale Bandbreite; maximale Verzögerung; vereinbarte Burst-Größe; vereinbarte Rate; Jitter; Fehler; Inhaberschaft; physikalische Position und Transportmedium.

8. Verfahren nach Anspruch 1, bei dem die Konfiguration des VPN-Tunnels die Auswahl eines bereits existierenden VPN-Tunnels einschließt, wobei der bereits existierende VPN-Tunnel zumindest einen Tunnel-Parameter erfüllt.

9. Von einem Diensteanbleter bereitgestelltes virtuelles privates Netzwerk-, PPVPN-, System, mit:

automatischen Erkennungseinrichtungen zur Verteilung von zumindest einem virtuellen privaten Netzwerk-, VPN-, Tunnel-basierten Parameter an zumindest ein erstes und ein zweites Diensteanbieter-Rand-PE-Gerät (102, 104); und
Tunnel-Signalisierungseinrichtungen zum Konfigurieren eines VPN-Tunnels (170) über einen Netzwerk-Backbone (106) zwischen den ersten und zweiten PE-Geräten zumindest teilweise auf der Grundlage des zumindest einen Tunnel-basierten Parameters.

10. System nach Anspruch 9, bei dem die automatische Erkennungseinrichtung so ausgebildet ist, dass sie den zumindest einen Tunnel-basierten Parameter als eine Erweiterung von zumindest einem automatischen Erkennungs-Protokoll verteilt.

11. System nach Anspruch 10, bei dem das automatische Erkennungs-Protokoll eines der folgenden Protokolle umfasst: einen Rand-Überleitungseinrichtungs-Protokoll-, BGP-, basierten Mechanismus; einen Domänen-Namensdienst-, DNS-, basierten Mechanismus; und einen Fernauthentifizierungs-Einwähl-Benutzerdienst-, RADIUS- basierten Mechanismus.

12. System nach Anspruch 9, bei dem die Tunnel-Signalisierungseinrichtung einen von folgenden Mechanismen einschließt: einen Ressourcen-Reservierungs-Protokoll-, RSVP-, basierten Mechanismus; einen Ressourcen-Reservierungs-Protokoll-Verkehrsauslegungs-, RSVP-TE-, basierten Mechanismus; einen Etlkettverteilungs-Protokoll-, LDP-, basierten Mechanismus; und einen Bedingungs-basierten Routenführungs-, LDP-CR-LDP-, basierten Mechanismus.

13. System nach Anspruch 9, bei dem der zumindest eine Parameter einen von folgenden Parametern einschließt: einen Typ des Tunnelungsmechanismus; zumindest einen PE-Tunnel-Endpunkt; zumindest ein Gemeinschafts-Routenziel; Topologie-Information; und zumindest einen Ressourcen-Parameter.

14. System nach Anspruch 13, bei dem der zumindest eine Ressourcen-Parameter einen von folgenden Parametern einschließt: minimale Bandbreite; ma-

ximale Verzögerung; vereinbarte Burst-Größe; vereinbarte Rate; Jitter; Fehler; Inhaberschaft; physikalische Position und Transportmedium,

15. System nach Anspruch 10 mit:

dem Netzwerk-Backbone; und
den ersten und zweiten PE-Geräten, die jeweils betriebsmäßig mit dem Netzwerk-Backbone verbunden sind.

Revendications

1. Procédé pour établir un tunnel de réseau privé virtuel VPN (170) entre un premier dispositif PE de bord de fournisseur (102) et un deuxième dispositif PE d'un PPVPN VPN géré par fournisseur (100) comprenant les étapes consistant à :

annoncer au moins un paramètre basé sur le tunnel à un ou plusieurs dispositifs PE sur un réseau fédérateur (106) en utilisant un mécanisme de découverte automatique, l'un ou les plusieurs dispositifs PE comprenant au moins l'un du premier dispositif PE et du deuxième dispositif PE ; et
configurer un tunnel VPN entre le premier dispositif PE et le deuxième dispositif PE sur la base au moins en partie de l'au moins un paramètre basé sur le tunnel.

2. Procédé selon la revendication 1, dans lequel le mécanisme de découverte automatique comprend l'un : d'un mécanisme basé sur le protocole de passerelle de frontière BGP ; d'un mécanisme basé sur le service de nom de domaine DNS ; et d'un mécanisme basé sur le service utilisateur de numérotation d'authentification à distance RADIUS.

3. Procédé selon la revendication 2, dans lequel l'au moins un paramètre basé sur le tunnel est distribué à l'un ou plusieurs dispositifs PE en tant qu'extension d'un protocole de découverte automatique.

4. Procédé selon la revendication 1, dans lequel la configuration du tunnel VPN comprend la configuration du tunnel VPN en utilisant au moins un mécanisme de signalisation de tunnel.

5. Procédé selon la revendication 4, dans lequel l'au moins un mécanisme de signalisation de tunnel comprend l'un : d'un mécanisme basé sur le protocole de réservation de ressource RSVP ; d'un mécanisme basé sur le protocole de réservation de ressource avec ingénierie de trafic RSVP-TE ; d'un mécanisme basé sur le protocole de distribution de label LDP ; et d'un mécanisme basé sur LDP avec routage à base de contraintes CR-LDP.

6. Procédé selon la revendication 1, dans lequel l'au moins un paramètre de tunnel comprend l'un de : un type de mécanisme de tunnelage ; au moins un point d'extrémité de tunnel PE; au moins une cible de routage de communauté ; des informations de topologie ; et au moins un paramètre de ressource.

7. Procédé selon la revendication 6, dans lequel l'au moins un paramètre de ressource comprend l'un de : bande passante minimale; délai maximal ; taille de rafale engagée ; débit engagé ; gigue ; erreur ; propriété ; position physique et support de transport.

8. Procédé selon la revendication 1, dans lequel la configuration du tunnel VPN comprend la sélection d'un tunnel VPN préexistant, le tunnel VPN préexistant étant conforme à l'au moins un paramètre de tunnel.

9. Système de réseau privé virtuel géré par fournisseur PPVPN comprenant :

des moyens de découverte automatique pour distribuer au moins un paramètre basé sur le tunnel de réseau privé virtuel VPN à au moins un premier et un deuxième dispositifs PE de bord de fournisseur (102,104) ; et
des moyens de signalisation de tunnel pour configurer un tunnel VPN (170) sur un réseau fédérateur (106) entre le premier dispositif PE et le deuxième dispositif PE sur la base au moins en partie de l'au moins un paramètre basé sur le tunnel.

10. Système selon la revendication 9, dans lequel les moyens de découverte automatique sont adaptés pour distribuer l'au moins un paramètre basé sur le tunnel en tant qu'extension d'au moins un protocole de découverte automatique.

11. Système selon la revendication 10, dans lequel le protocole de découverte automatique comprend l'un : d'un mécanisme basé sur le protocole de passerelle de frontière BGP ; d'un mécanisme basé sur le service de nom de domaine DNS ; et d'un mécanisme basé sur le service utilisateur de numérotation d'authentification à distance RADIUS.

12. Système selon la revendication 9, dans lequel les moyens de signalisation du tunnel comprennent l'un : d'un mécanisme basé sur le protocole de réservation de ressource RSVP ; d'un mécanisme basé sur le protocole de réservation de ressource avec ingénierie de trafic RSVP-TE ; d'un mécanisme basé sur le protocole de distribution de label LDP ; et d'un mécanisme basé sur LDP avec routage à base de contraintes CR-LDP.

13. Système selon la revendication 9, dans lequel l'au moins un paramètre de tunnel comprend l'un de : un type de mécanisme de tunnelage ; au moins un point d'extrémité de tunnel PE ; au moins une cible de routage de communauté ; des informations de topologie ; et au moins un paramètre de ressource.

14. Système selon la revendication 13, dans lequel l'au moins un paramètre de ressource comprend l'un de : bande passante minimale ; délai maximal ; taille de rafale engagée ; débit engagé ; gigue ; erreur ; propriété ; position physique et support de transport.

15. Système selon la revendication 10 comprenant :

le réseau fédérateur ; et
le premier et le deuxième dispositifs PE chacun connecté de manière utilisable au réseau fédérateur.

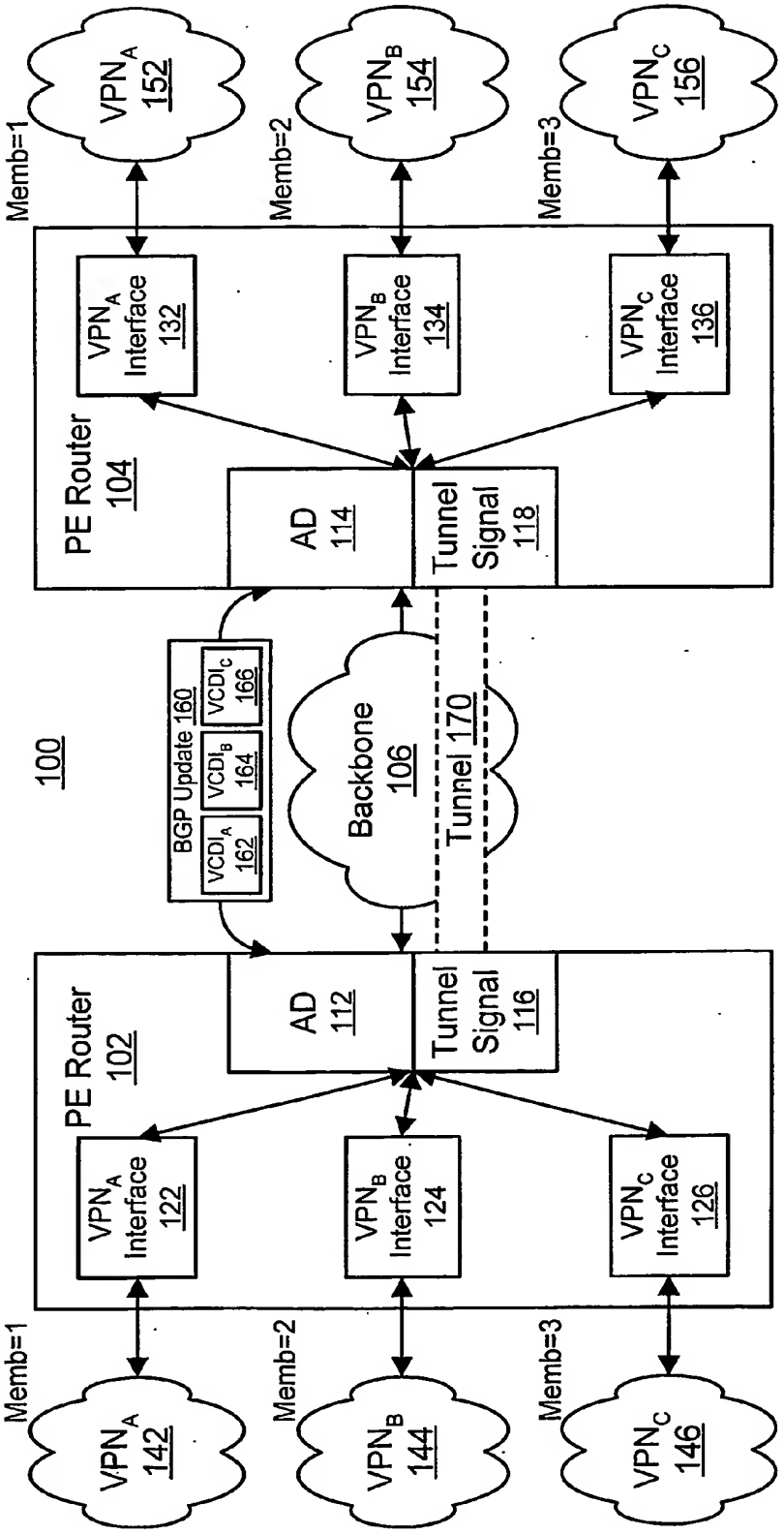
100
PE Router 102
AD 112
Tunnel Signal 116
VPN_A Interface 122
VPN_B Interface 124
VPN_C Interface 126
Memb=1
Memb=2
Memb=3
VPN_A 142
VPN_B 144
VPN_C 146
Backbone 106
Tunnel 170
BGP Update 160
VCDI_A 162
VCDI_B 164
VCDI_C 166
PE Router 104
AD 114
Tunnel Signal 118
VPN_A Interface 132
VPN_B Interface 134
VPN_C Interface 136
VPN_A 152
VPN_B 154
VPN_C 156

Fig. 1

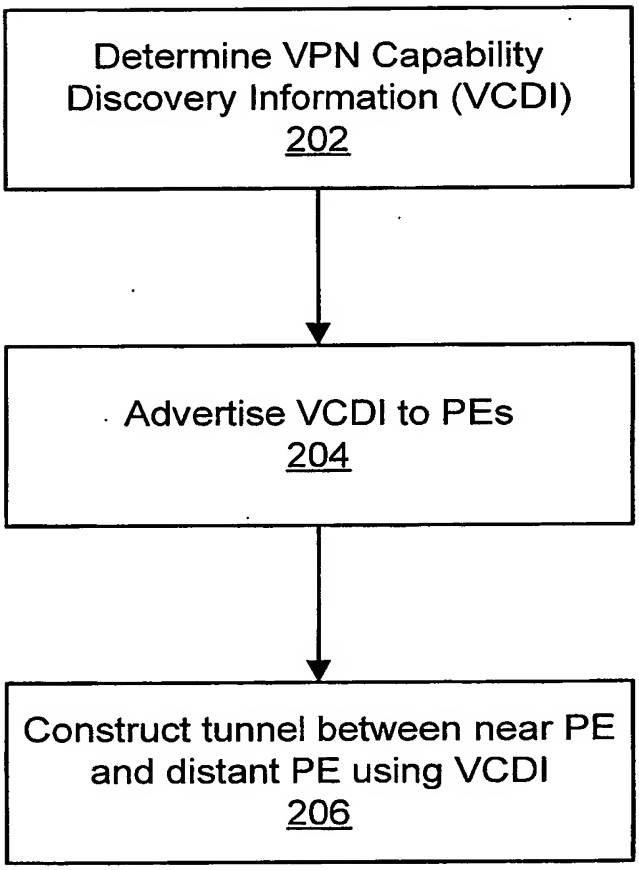
Determine VPN Capability Discovery Information (VCDI)
202
Advertise VCDI to PEs
204
Construct tunnel between near PE and distant PE using VCDI
206
200

Fig. 2

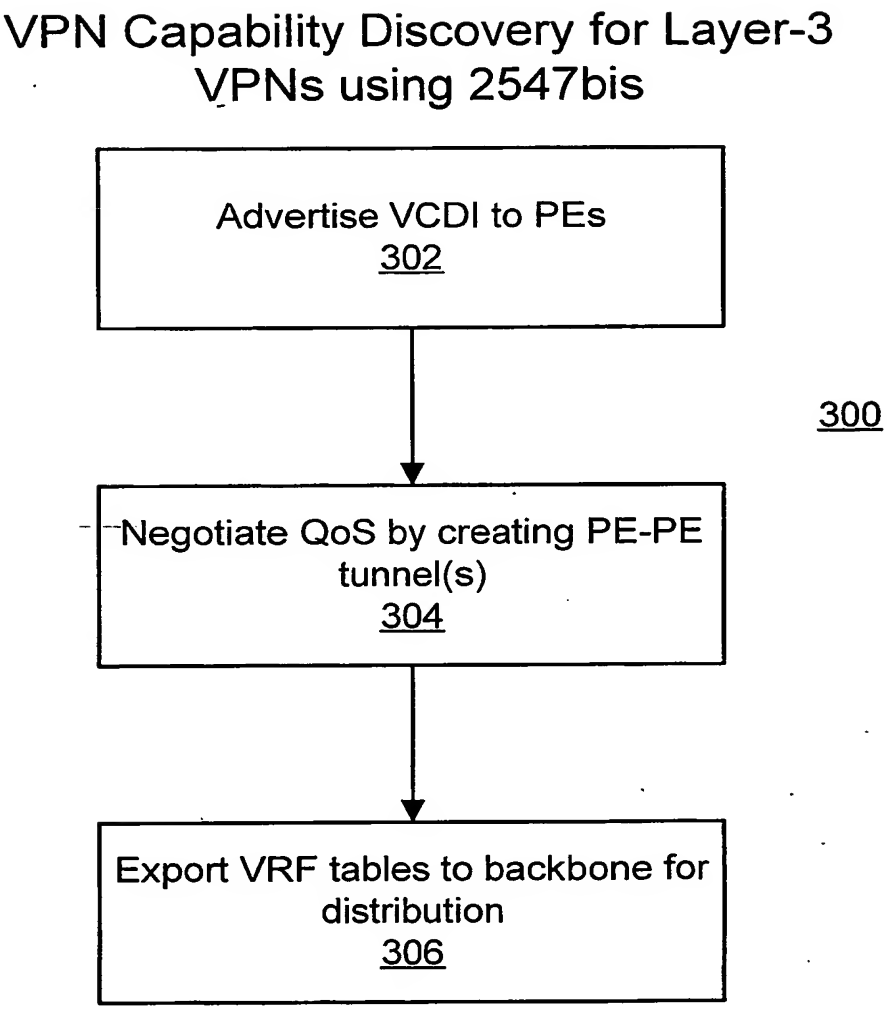
VPN Capability Discovery for Layer-3 VPNs using 2547bis
Advertise VCDI to PEs
302
300
Negotiate QoS by creating PE-PE tunnel(s)
304
Export VRF tables to backbone for distribution
306

Fig. 3

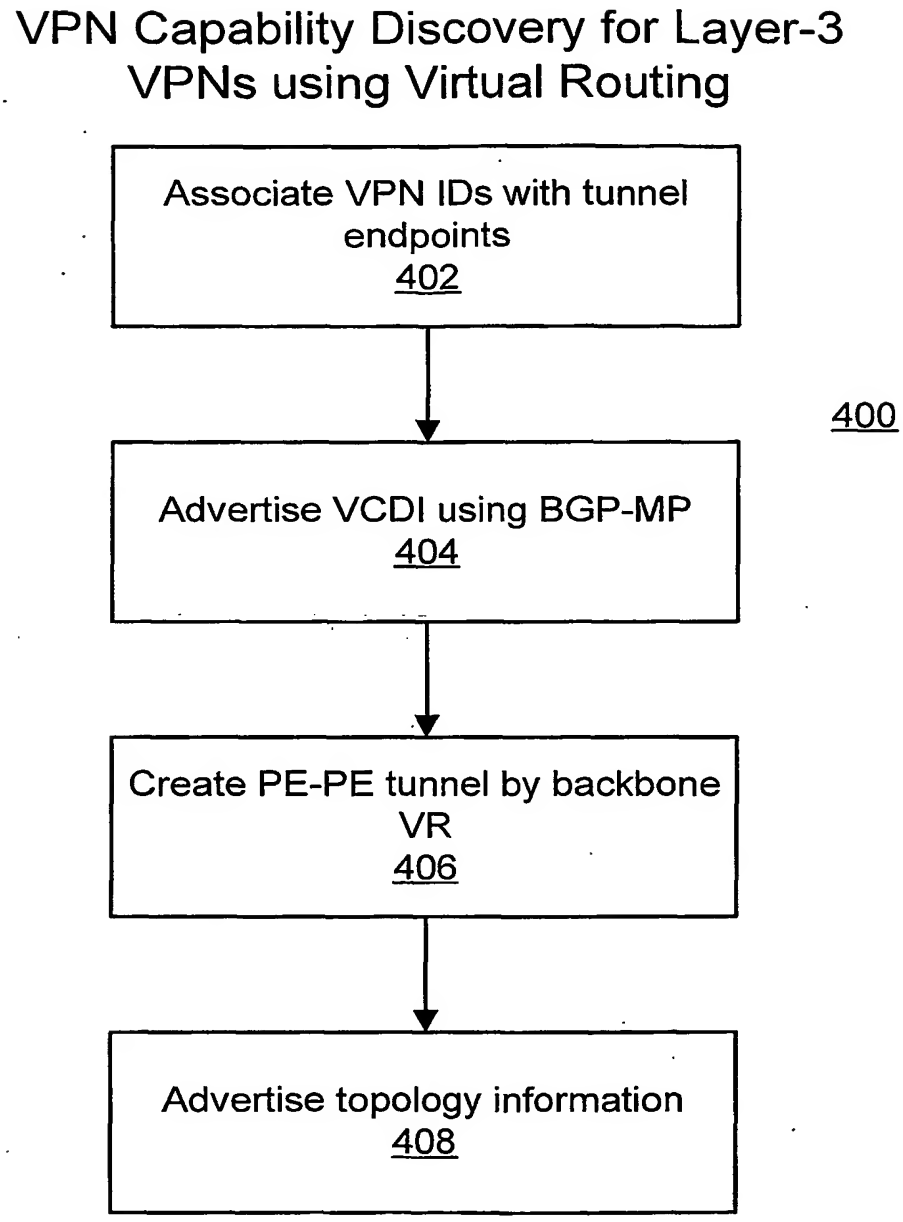
VPN Capability Discovery for Layer-3 VPNs using Virtual Routing
Associate VPN IDs with tunnel endpoints
402
400
Advertise VCDI using BGP-MP
404
Create PE-PE tunnel by backbone VR
406
Advertise topology information
408

FIG. 4

VPN Capability Discovery for Layer-2 VPNs using VPLS or VPW

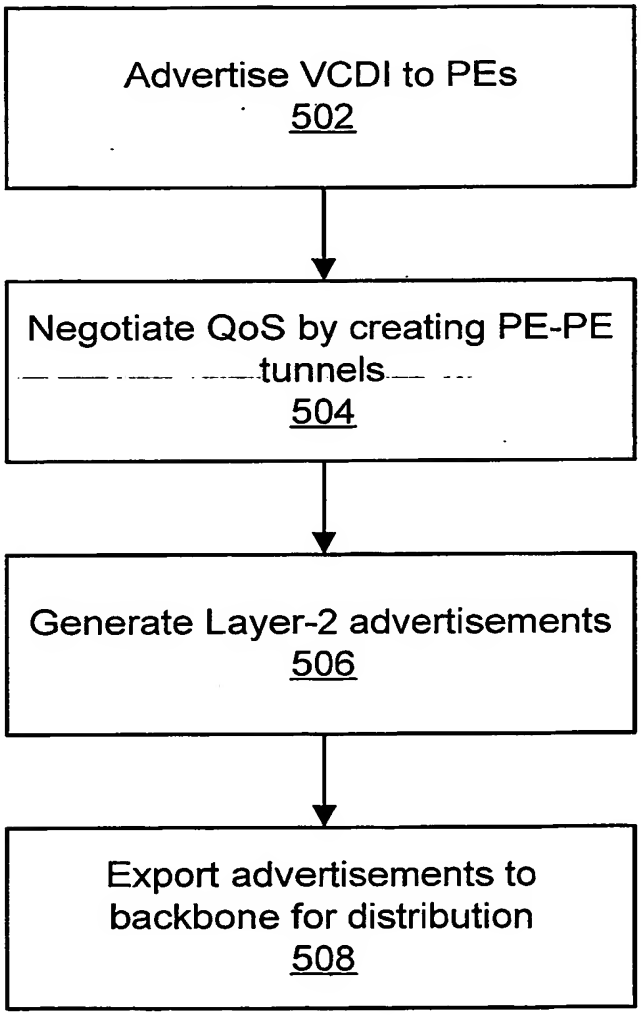

Fig. 5